**Quay Route to PASSTHROUGHT**

<https://docs.redhat.com/it/documentation/red_hat_quay/3.11/html/deploying_the_red_hat_quay_operator_on_openshift_container_platform/configuring-traffic-ingress#creating-config-bundle-secret-tls-cert-key-pair>

**Insecure Registy add to Cluster / Allowing insecure registries**

<https://docs.openshift.com/container-platform/4.14/openshift_images/image-configuration.html#images-configuration-insecure_image-configuration>

**Image policy prevents the creation of samples-operator imagestreams after upgrading to OCP 4**

<https://access.redhat.com/solutions/6547281>

**Firewall changes for container image pulls**

[Firewall changes for container image pulls - Red Hat Customer Portal](https://access.redhat.com/articles/6999582)

https://access.redhat.com/articles/6999582

**How to change the global pull secret in OCP 4**

[How to change the global pull secret in OCP 4 - Red Hat Customer Portal](https://access.redhat.com/solutions/4902871)

https://access.redhat.com/solutions/4902871

**OSD prepare pod stuck in init 0/2 with event rpc error: code = AlreadyExists**

[OSD prepare pod stuck in init 0/2 with event rpc error: code = AlreadyExists - Red Hat Customer Portal](https://access.redhat.com/solutions/7053855)

<https://access.redhat.com/solutions/7053855>

* Gestione utenza tecnica o robot account

Secondo best practices è consigliato usare il robot account.

I robot account hanno permessi limitati e possono essere configurati con accessi specifici per singole attività.

È più semplice tracciare e monitorare le attività dei robot account rispetto ad un account utente globale.

[https://docs.redhat.com/it/documentation/red\_hat\_quay/3.11/html-single/use\_red\_hat\_quay/index#user-org-intro\_use-quay](https://urldefense.com/v3/__https:/docs.redhat.com/it/documentation/red_hat_quay/3.11/html-single/use_red_hat_quay/index*user-org-intro_use-quay__;Iw!!OrxsNty6D4my!9f6BpPZQXJJkr9i_4Y2lQ4pNo9Gfisyw5MJlM9aUhTHj--9CddTiPPTYW8krtIHhSoCv92ZCgI6GzXB3ZlBD8k4$)

In alternativa ho consigliato di creare un'utenza tecnica con permission limitate da impostare in pipeline di pre-check, e poi il robot account (Creato in automazione dall’utenza tecnica) per le operazioni di push / pull / build etc…

Si verificherà anche con sicurezza quale sia la strada più adatta.

* Gestione sync ldap e team in quay

Si vuole configurare LDAP in quay e gestire anche gli utenti LDAP e gli utenti locali all'interno dei Teams e delle Organizations. Ad eccezione di eventuali conflitti a livello di permission è possibile effettuare tale configurazione. Dove possibile si può utilizzare anche l'accesso tramite Oauth OpenShift che risulta già configurato, in quanto in OpenShift è già stato configurato LDAP con dei sync specifici.

* TLS termination in quay

Custom certificate per quay: Al momento la route di quay è configurata con il certificato self-signed dell'ingress \*.apps è possibile definire un custom certificate.

Per farlo bisogna impostare unmanaged il kind TLS nella configurazione di quay e configurare una secrets con certificato e ca ed infine definire la rotta come Passthrough.  
  
[https://docs.redhat.com/it/documentation/red\_hat\_quay/3.11/html/deploying\_the\_red\_hat\_quay\_operator\_on\_openshift\_container\_platform/configuring-traffic-ingress#operator-preconfig-tls-routes](https://urldefense.com/v3/__https:/docs.redhat.com/it/documentation/red_hat_quay/3.11/html/deploying_the_red_hat_quay_operator_on_openshift_container_platform/configuring-traffic-ingress*operator-preconfig-tls-routes__;Iw!!OrxsNty6D4my!9f6BpPZQXJJkr9i_4Y2lQ4pNo9Gfisyw5MJlM9aUhTHj--9CddTiPPTYW8krtIHhSoCv92ZCgI6GzXB3mHz75kw$)